Are Public Records Too Public? Why Personally Identifying Information Should Be Removed from Both Online and Print Versions of Court Documents

KRISTEN M. BLANKLEY*

In recent years, judicial districts have begun to place many of their public records on the Internet in searchable databases. Prior to Internet publication, sensitive material contained in court documents was protected by the phenomenon of "practical obscurity." Today, however, many of the documents are available online are exact replicas of the documents submitted to the courts—complete with social security numbers, addresses, phone numbers, credit card numbers, bank account numbers, tax information, and the private details of many people's lives. With this information available at the click of a mouse, the government increase the risk of identity theft or other misuse of this sensitive information. In order to curb these problems, this Note urges legislatures to enact statutes prohibiting the online publication of personally identifying information. These statuses, though, should place a burden on lawyers, and not the courts, to remove this information from court documents. Such legislation should help curb the amount of personal information on the Internet while holding attorneys responsible for safeguarding the interests of their own clients.

I. INTRODUCTION

A simple Internet search through an online judicial docket could reveal highly personal information, such as an individual's address, medical records, criminal involvement, or even social security number.[1] Litigants' expectation of privacy in that information has become an important issue since federal and state

---

* B.A., Hiram College, 2001; J.D., The Ohio State University Moritz College of Law, 2004 (expected). I would like to thank Professors Peter Swire and Sarah Cole for their helpful comments on earlier drafts of this Note. Thanks, also, to Jennifer Caouette for making me aware of this problem in Ohio and throughout the country. Special thanks to my husband, Mike, and to my parents, Richard and Susan, for all of their love and support during the writing and editing processes.

[1] *See, e.g.*, Rebecca A. Askew, *Courts Debate Electronic Access: How Much Is Too Much?*, CHI. DAILY LAW BULL., Oct. 8, 2002, at 5 (threat of criminal intent of some of the Internet viewers gives rise to debate over the appropriate amount of access); Carrie Kirby, *Intimate Details: Credit card, Social Security Numbers and Other Data Left Open to Prying Eyes when Court Documents are Posted Online*, S. F. CHRON., Mar. 15, 2001, at B1 (as courts place more private information online, risk to invasion of privacy is heightened); Liz Sidot, *Internet Prompts Governments to Revisit Open Records*, CHATTANOOGA TIMES FREE PRESS, Oct. 15, 2002, at E1 (because of the severe consequences of the possibility of identity theft through access to online court documents, many states are debating their laws and policies).

governments began to make available a myriad of public documents online, ranging from agency rulings[2] and property deeds[3], to sex-offender registration[4], and court filings.[5] The last of these categories, court documents, appears to be the most controversial and the biggest threat to privacy. Many of these public documents contain personal, even intimate, information, including social security numbers, bank accounts, medical records, trade secrets, and criminal records.[6] The specific categories of documents published online include civil court filings,

---

[2] *See, e.g.*, National Labor Relations Board, *Decisions and Orders of the NLRB*, *at* http://www.nlrb.gov/nlrb/shared_files/decisions/board.asp (last visited Jan. 22, 2004) (maintaining a comprehensive listing of decisions and orders dating back to September 1984); Federal Trade Commission, *Adjudicative Proceedings*, *at* http://www.ftc.gov/os/adjpro/index.htm (last visited Jan. 22, 2004) (making available online selected adjudicative orders dating back to September 1996); *see also* United States Government Printing Offices, *Administrative Decisions*, *at* http://www.access.gpo.gov/index.html (making available decisions from various administrative agencies, including the Merit Systems Protection Board and the GAO Comptroller General).

[3] Counties such as Broward and Palm Beach in Florida have scanned property deeds into the counties' searchable databases. Jon Burstein & Paula McMahon, *Social Security IDs Reach Internet; Numbers Appear in Public Documents on Government Sites*, S. FLA. SUN-SENTINEL, Apr. 18, 2002, at 1A. Many of these deeds include the social security numbers of the holders, as is required by Florida law. *Id.* For further discussion of Florida's mandate to place public documents on the Internet, see *infra* Section III.B.2.

[4] Alaska is one of a number of states that posts the names of convicted sex-offenders online under variations of "Megan's Law," requiring states to notify local residents when a convicted sex-offender moves to the neighborhood. The Internet has proven to be a quick and convenient way to disseminate this information. *Public Records in Public View—Online?*, BUS. WEEK ONLINE, *at* http://www.businessweek.com/technology/content/Oct2002/tc20021029_1516.htm (Oct. 29, 2002). The Alaska Sex Offender Registration Act specifically allows for law enforcement officials to publish this information in an electronic format to be used by "any person for any purpose." *Id.* Alaska's registry can be viewed online at http://www.dps.state.ak.us/nSorcr/asp/. All but thirteen states in the United States maintain statewide online registries. The FBI maintains a complete list of available online databases and links to those databases at http://www.fbi.gov/hq/cid/cac/states.htm.

[5] The federal government has a comprehensive collection of court documents online and available to the public. The collection, known as PACER (Public Access to Court Electronic Records), can be accessed at http://pacer.psc.uscourts.gov. For further discussion of PACER, see *infra* Section III.A. In addition, individual district courts have been authorized to place bankruptcy and civil case filings online; however, criminal cases are not yet available for Internet publication. *See* Andy Sullivan, *Some U.S. Court Data Will Be Posted Online*, THE SAN DIEGO UNION-TRIB., Sept. 25, 2001, at 11. State governments have allowed a varying degree of access to court documents online. For a listing of each state's open record laws, see *infra* note 68.

[6] *See, e.g.*, Askew, *supra* note 1 (threat of criminal intent of some of the Internet viewers gives rise to debate over the appropriate amount of access); Kirby, *supra* note 1 (as courts place more private information online, risk to invasion of privacy is high); Sidot, *supra* note 1 (because of the severe consequences of the possibility of identity theft through access to online court documents, many states are debating their laws and policies).

bankruptcy filings, criminal documents, opinions (both "published" and "unpublished"), and even attorneys' briefs and motions.[7]

Because of the potential invasion of privacy, constitutional issues lurk in the background. Thus far, no state's highest court has issued a constitutional ruling on this issue.[8] Although the Federal Constitution does not explicitly mention a right to privacy, the Supreme Court has acknowledged such a right.[9] Ten state constitutions, in contrast, do specifically grant a right to privacy.[10] Despite any federal or state rights of privacy, open access laws are often read broadly[11]

---

[7] *See* Judge Nancy Gertner, *Electronic Case Filing Is Here to Stay*, 46 B. B. J. 8 , 8 (2002) (due to the rise in electronic filing, court documents are already online and then placed in a database available for public access); Sherri M. Owens, *Point-and-Click Your Way to Criminal-Case Information; Visitors to the Clerk of Courts Site Can Learn About Charges, Court Dates, and the Parties Involved*, THE ORLANDO SENTINEL, July 23, 2002, at G3 (Lake County, Florida publishes both civil and criminal court documents, excepting only family, juvenile, and probate cases); Joel Rothman, *Privacy in Federal Court Web Sites?*, MIAMI DAILY BUS. REV., May 9, 2001 (districts, such as the Southern District of Florida, are putting entire civil case files online, including pleadings, briefs, and rulings on motions); Sullivan, *supra* note 5 (the Judicial Conference of the United States approved of district courts posting civil and bankruptcy files). Other searchable databases, such as westlaw.com, lexis.com, and findlaw.com, are generally limited to judicial opinions and Supreme Court briefs, and do not usually include other parts of a civil case, such as rulings on motions and lower-court briefs.

[8] A few lower courts have addressed the issue; however, each of them rejected constitutional attacks to the placing of public records on the Internet. *See, e.g.*, Kallstrom v. City of Columbus, 165 F. Supp. 2d 686, 695 (S.D. Ohio 2001).

> Anyone with an individual's name and either Internet access or the initiative to visit a local government office can scan county property records, court records, or voter registration records for such information as an individual's address, the exact location of his or her residence, and even a floor plan of the home.

Id.; *see also* Doe v. City of New York, 201 F.R.D. 100, 102-03 (S.D.N.Y. 2001) (attorney may not proceed as "Jane Doe" out of fear of reputational injury in a criminal lawsuit when the case is available via online databases); State v. Stevens, 992 P.2d 1244, 1249 (Kan. Ct. App. 1999) (Internet availability of sex-offender registration is not unconstitutional).

[9] *See generally* Griswold v. Connecticut, 381 U.S. 479 (1965); Eisenstadt v. Baird, 405 U.S. 438 (1972); Roe v. Wade, 410 U.S. 113 (1973); Nixon v. Warner Communications, Inc., 435 U.S. 589 (1978); *see infra* Section IV.

[10] *See* ALASKA CONST. art. I § 22; ARIZ. CONST. art. II § 8; CAL. CONST. art. I § 1; FLA. CONST. art. I § 23; HAW. CONST. art. I §§ 6–7; ILL. CONST. art. I § 6; LA. CONST. art. I § 5; MONT. CONST. art. II § 10; S.C. CONST. art. I § 10; WASH. CONST. art. I § 7.

[11] The Ohio Supreme Court is one of many courts that construe public records acts liberally. *See, e.g.*, Consumer News Serv., Inc. v. Worthington City Bd. of Educ., 776 N.E.2d 82, 88 (Ohio 2002) ("[W]e must liberally construe [the Public Record Act] in favor of broad access and resolve any doubt in favor of disclosure of public records.") Other states also use similar language in interpreting open records laws. *See, e.g.*, Wichita Eagle and Beacon Publ'g Co. v. Simmons, 50 P.3d 66, 82 (Kan. 2002); Landis v. Moreau, 779 So. 2d 691, 694–95 (La. 2001); Kirwan v. The Diamondback, 721 A.2d 196, 203 (Md. 1988); Miss. Dep't of Wildlife,

because any privacy interest in the information contained in court documents is overshadowed by the governments' interest in keeping records open.

This Note will discuss the extent to which federal and local governments have created online access for court documents and the public's reaction to this increase in access. Section II will examine the debate surrounding the increasing use of the Internet to access court documents, evaluating the pros and cons of online access. Section III will examine the steps taken by the federal government in putting documents online, as well as explore three states with particularly extensive public access laws or databases. Federal and state constitutional issues will be discussed in Section IV, and the most commonly proposed solutions to the problem of invasion of privacy will be identified in Section V. This note will prove, in Section VI, that a statutory scheme requiring lawyers to redact personally identifying information from court documents in both print and electronic form, and including the imposition of civil liability for lawyers who fail to comply, is the most effective solution to the privacy problem.

II. WHY "PUBLIC" IS TOO PUBLIC

Widespread Internet dissemination of court documents increases the vulnerability of those whose personal and embarrassing information may become available to anyone with an Internet connection. Thus, a balance must be struck between protecting a person's sensitive information and the public's right to know the workings of the judicial system. The rise in Internet access to public documents has spawned debate questioning how available public documents ought to be, and whether public documents should be available at both the local courthouse and across the nation—or the world—at the click of a mouse. These questions have divided scholars and practitioners into two groups: those in strong support of Internet access of court documents, and those who strongly disagree. There seems to be little intermediate ground.[12] Although each side is armed with policy reasons, those in favor of a more expansive right to informational privacy appear to have the upper hand because a litigant's interest in privacy of sensitive information outweighs the interest in making this specific information public.

Fisheries, and Parks v. Miss. Wildlife Enforcement Officers' Ass'n, 740 So. 2d 925, 936 (Miss. 1999); Finberg v. Murnane, 623 A.2d 979, 981 (Vt. 1992); Limstrom v. Ladenburg, 963 P.2d 869, 873 (Wash. 1998); Pagel v. Franscell, 57 P.3d 1226, 1233 (Wyo. 2002).

[12] *See* Marc Davis, *Do You Want Your Divorce on the Web?; Lawyers Debate How Much Info Should Be Aired*, THE VIRGINIAN-PILOT, Feb. 9, 1997, at J1; (showing the conflict between having a right to view public records and the exposure that citizens face when their private information is placed online); Kiran Krishnamurthy, *ACLU: Take Personal Information Off Net*, THE RICHMOND TIMES-DISPATCH, Oct. 2, 2002, at B-2 (the ACLU, while advocating public disclosure, urges for removal of personal information from public records before they are available online); Daniel C. Vock, *Online Access to Court Records Sparks Debate*, CHI. DAILY LAW BULL., Feb. 6, 2001, at 1 (although privacy rights advocates want to keep this information from the Internet at all costs, the news media urges for increased public disclosure).

Although court documents have always been considered public documents,[13] they were relatively inaccessible.[14] A person interested in a particular court record had to travel to the local courthouse, ask the local reporter where to find the document, and pay for copying costs.[15] This method of access was open for those who took the time to obtain the paper copy of the desired document(s). The Internet, however, has irreversibly changed the means by which court documents can be disseminated.

A. *Policies for Increased Privacy Protections*

Privacy advocates urge that private information be prohibited from online disclosure for four reasons: (1) the dissemination of private information increases the risk of identity theft; (2) employers and renters may use this information in a discriminatory manner; (3) private family information could subject individuals to embarrassment; and (4) attorneys may employ tactics to protect client information rather than to win a case, resulting in less zealous representation.

---

[13] *See* Hon. Lewis A. Kaplan, *Litigation, Privacy and the Electronic Age*, 4 YALE SYMP. L. & TECH. 1, at II (2001) *at* http://research.yale.edu/lawmeme/yjolt/modules.php?name=News&file=article&sid=5 ("Court records long have been presumptively open to public inspection.").

[14] *See* U.S. Dep't of Justice v. Reporters Comm., 489 U.S. 749, 780 (1989) (public information can retain a "practical obscurity" character if kept in remote places); *see also* Peter Piazza, *How Public Should Public Records Be?*, SECURITY MGMT., Apr. 1, 2001. Piazza commented on "practical obscurity," and in his opinion:

> You might think that there's nothing practical about obscurity, but "practical obscurity" has long been a legal concept. It means that records made public in connection with a court case remain, for all practical purposes, obscure because they are difficult to access. They are located in courthouses around the country, available only to those who travel to where they are.

Id. The rise of the Internet has dramatically changed this old practice by allowing anyone with an Internet connection to search court records in their own homes, anywhere in the world. Judge Kaplan, too, believes that the "practical obscurity" of documents in courthouses secured the privacy rights of the individual litigants for two reasons: First, most discovery activities took place between the two lawyers without being placed in the public record. And, second, the media only focused its attention on trials that generated mass public interest. *See* Kaplan, *supra* note 13, at II; *see also* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1139 (2002) ("For a long time, public records were only available locally. Finding information about a person often involved a treasure hunt around the county to a series of local offices to dig up records.").

[15] *See* Askew, *supra* note 1. Presumably, those with a "bad" intent would hesitate to "get in a car, travel to the courthouse, head to the clerk's office and obtain the correct file to snoop or gather information for the illegal purpose." *Id.* Internet access and searchable databases, though, have created a situation in which these actors need not leave their houses or even know the future victims before they attempt to obtain records. *Id.*

Identity theft is one of the fastest growing crimes in America.[16] Placing court documents online containing personally identifiable information would make the commission of this crime easier. Identity theft is defined as "the unlawful use of another person's identifying information to commit fraud."[17] The advent of the Internet has greatly increased the incident rate of this crime.[18] Because the personally identifying information in court documents is rarely removed before a document is posted online,[19] courts have created a substantial risk of identity theft for those whose records are exposed to the public.[20]

---

[16] *See, e.g.*, Jeff Sovern, *The Jewel of Their Souls: Preventing Identity Theft Through Loss Allocation Rules*, 64 U. PITT. L. REV. 343, 344 n.5 (2003) (citing sources stating that between 500,000 and 700,000 people are victims of identity theft each year and that this number is one the rise).

[17] ALAN CHARLES RAUL, PRIVACY AND THE DIGITAL STATE: BALANCING PUBLIC INFORMATION AND PERSONAL PRIVACY 13 (2002). Although identity fraud can occur in a myriad of ways, the most common ones include credit card fraud, bank fraud, or the unauthorized establishment of telephone, cellular, or other utility accounts. *Id.* (citing Betsy Broder, Fed. Trade Comm'n, Prepared Statement of the Federal Trade Commission on Identity Theft Before the Committee on Banking and Financial Services, United States House of Representatives (Sept. 13, 2000), *available at* http://www.ftc.gov/os/2000/09/idthefttest.htm). This crime harms both the individual and the credit card companies or other businesses. *Id.* at 13–14. The individual victim may have emotional consequences, such as anger, and financial consequences, such as trouble securing a new credit card or bank loan. The lending institutions are affected because they usually absorb any monetary loss. *Id.* at 14. Identity fraud is currently regarded as "the fastest growing financial crime in the [United States]." *Id.* at 61.

[18] *See id.* at 14. Identity theft imposes a cost on consumers alone of up to $100 million each year. *See* Mark Grossman, *The Other You: The Misery of Identity Theft*, BROWARD DAILY BUS. REV., Sept. 4, 1998, at B1. Reports show that the dollar value of identity theft cases has doubled in the past few years and that the number of fraud cases reported to the Social Security Administration has increased threefold. Kathy M. Kristof, *New Law to Assist Victims in Fight Against Identity Fraud*, L.A. TIMES, Oct. 31, 1998, at C1. Furthermore, credit reporting firms indicate that fraud reports have jumped from less than 12,000 reports in 1992 to over 50,000 reports in 1998. *Id.*; *see* Kurt M. Saunders & Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 CORNELL J.L. & PUB. POL'Y 661 (1999) for an overview of the identity theft problem and ways to alleviate the problem; *see also, e. g.*, Stephanie Byers, Note, *The Internet: Privacy Lost, Identities Stolen*, 40 BRANDEIS L.J. 141 (2001) (outlining the problems of identity theft and comparing federal, state, and international solutions).

[19] Florida, by statute, must make available all public documents—new and old—in an online format by the year 2006. To accomplish this goal, local courts were merely scanning in old records without removing social security numbers and other personally identifiable information. Burstein & McMahon, *supra* note 3. For further discussion, see *infra* notes 87–91 and accompanying text. However, because of the sensitive nature of the information being placed online, the Florida Supreme Court issued a temporary moratorium on placing certain court information online. *See infra* notes 92–97 and accompanying text.

[20] Catching the perpetrators of identity theft is difficult, so it is hard to determine exactly where the wrongdoers procured their information. At least one crime ring admitted to using PACER, the federal online database, in order to secure personal information about prisoners in

Widespread dissemination of public documents could create the situation in which employers and landlords use this information in a discriminatory manner.[21] When employers and landlords process applications, they usually submit a social security number to a credit-reporting agency. These credit agencies must comply with the Fair Credit Reporting Act; employers and landlords who do independent searches are not similarly bound.[22] Employers and landlords could then use this information to unlawfully refuse employment or housing.[23]

Publishing family law documents with details about divorce, child custody, or probate matters could subject individuals to embarrassment or public shame..[24] A couple in the middle of a divorce proceeding may not only expose the intimate details of their relationship, but also might reveal the intimate details of their financial position.[25] In order to alleviate this risk of embarrassment, family law

---

order to open false bank and credit accounts. The seven involved in this conspiracy that victimized thirty-four prisoners and twenty financial institutions were indicted in February 2003. Elaine Silvestrini, *Federal Prisoners' Personal Information Used in Credit Fraud*, THE TAMPA TRIB., Feb. 8, 2003, at 3; *Seven Charged with Stealing IDs of Inmates*, THE TALLAHASSEE DEMOCRAT, Feb. 9, 2003, at B10.

[21] *See* Kirby, *supra* note 1.

[22] *Id.* Furthermore, when a person is not granted employment or housing, the employer or the renter must disclose the investigation to the individual. Additionally, the individual has a legal right to receive a copy of the report used in making the employment or housing decision. *Id.*

[23] One Cincinnati man, Jim Moehring, became quite familiar with the pros and cons of Internet dockets. As an employer, he used the Hamilton County, Ohio website to look up potential hirees, and he turned some away based on the information that he found. However, he was later the victim of identity theft when someone used his social security number to charge over $11,000 fraudulently. Meohring's social security number was on a traffic ticket that was placed online. *Online Court Records Quandry*, THE CINCINNATI POST, Oct. 10, 2002, at A1.0. Traffic tickets are public records in Ohio. However, Ohio law does not permit redaction of sensitive materials before records are placed online. See *infra* section III.B.1 for a discussion on Ohio public record laws.

[24] Davis, *supra* note 12. As part of the debate, Virginia lawyer Richard J. Byrd posed the following hypothetical:

> I know my neighbor is in a divorce fight with her husband and I'm a curious type, so I just log on and scope out her divorce file. WOW! Some really juicy stuff there. Why, I never realized that she and the president of our homeowner's association were having an affair. And it is really interesting to read that she accuses her husband of selling child porn on the WWW (World Wide Web) . . . .

Id. The details of a divorce need not be as dramatic as in this hypothetical for individuals to be concerned. It is arguable that in even the most typical of dissolutions, the participants would not want the public to know the particulars of their relationship.

[25] Divorce, child custody, and probate matters always contain some financial information. This information is necessary to determine the amount of spousal support due, the appropriate amount of child support, or how to manage an estate. *See, e. g.*, Stephen Hudak, *Public vs. Private: Issue is a Cloudy One; Weatherman Dick Goddard Asks Judge to Keep Heated*

matters could be treated like most juvenile records by only publishing the initials of participants, rather than full names.[26] Under this system, the documents are still public, and only the names are removed.

Finally, placing sensitive and personally identifying information in court records accessible through the Internet could change the tactics of litigants and attorneys. For instance, litigants could threaten to use the other party's highly personal information in court documents, knowing that they would be available for Internet dissemination.[27] In a divorce action, one spouse could easily threaten to place in court documents financial information spanning the life of the marriage in order to better a settlement position.[28] In contrast, with the increasing number of documents available by the Internet, both the litigant and the lawyer

---

Divorce Case Sealed, THE CLEVELAND PLAIN DEALER, Dec. 18, 2003, at B1 (stating that it would be easy for someone to look up a neighbor's divorce papers on the Internet, and those papers usually include bank account information and social security numbers); Bill Sloat, *Web Stirs Debate on Public Records: Issues of Privacy More Urgent with Ease of Access*, THE CLEVELAND PLAIN DEALER, Mar. 17, 2002, at B1 (noting that, on the various Ohio court websites, information concerning annual income, payment of child support, and amount of alimony are available).

[26] *See, e.g.*, ALASKA STAT. § 47.12.300(c) (Michie 2002) (disclosure of a minor's name is generally not permissible in delinquency charges); ARIZ. REV. STAT. § 8-807(P) (1999) (minor's name shall not be disclosed in any records, including court records, that pertain to child abuse); CAL. PENAL CODE § 11167.5 (2000) (agencies should redact names of juveniles from records when required by law to maintain confidentiality); COLO. REV. STAT. § 13-8-124 (2002) (juvenile matters on appeal should only list the initials of the juvenile); GA. CODE ANN. § 35-3-40 (2002) (juvenile records may be maintained without full name of juvenile); N.J. STAT. ANN. § 2A:82-46(a) (1994) (in child abuse cases, names of children should be replaced with initials). The argument has been made that divorce and other family law records should be open in order for the public to understand how the court system operates. *Electronic Access to Court Records: Ensuring Access in the Public Interest*, NEWS MEDIA & L., Oct. 1, 2002, at 25, 28. However, merely substituting initials for real names and redacting social security numbers would still allow observers to determine how the court system operates.

[27] *See* Jennifer Greene, *Competing Interests Regarding Electronic Court Records: Privacy versus Open Access in Arizona*, 40 JUDGES' J. 26, 27–28 (No. 3 2001). In light of this and other concerns, the Arizona committee studying the effects of placing court documents online ultimately recommended that personally identifiable information—social security numbers, credit card numbers, and other financial numbers—not be present on the Internet versions of the case records. If this information is relevant to the disputed issues in the case, this information would be maintained on a separate "sensitive information form" available at the court with the other paper documents. *Id.* at 28. The committee believes that the "practical obscurity" phenomenon would prevent sensitive information from widespread dissemination. *Id.*

[28] James Cissell, former clerk of courts for Hamilton County, Ohio, noted that the tax returns of a "Hall of Fame" sports figure are currently available on the county's website because his wife included them in her court filings. James Cissell, *Privacy and Court Records on the Internet: Mutually Exclusive Concepts*, 40 JUDGES' J. 29, 29 (No. 3 2001). For more information on the Hamilton County court website, see *infra* notes 76–82 and accompanying text.

must be very aware of the contents of their own briefs, motions, pleadings, and other documents.[29] As a result, a lawyer may be less zealous in her representation in order to protect her client's sensitive information.[30] By eliminating the use of personally identifiable information from all court documents, the resolution of cases would turn not on threats of public embarrassment and exposure, but on legal issues.[31]

B. *Increased Access Policies and Their Shortcomings*

Proponents of increased access advocate three primary reasons for maintaining copies of public documents online: (1) that "public" means public, no matter the forum, (2) that the public records are essential for good reporting, and (3) the accessibility of records will save lawyers time and money.[32] Each of these reasons, while plausible, is flawed.

Those in support of increased access to public documents argue that the records are public documents and that posting them is a new forum for dissemination of the public information.[33] They believe that, because the public

---

[29] When the Northern District of Georgia began to make civil filings available via PACER, a letter was distributed to over 11,000 attorneys, cautioning them to be "very careful[ ] before filing any document with the court because that document, once filed, will be available on the Internet." R. Robin McDonald, *Northern District Puts Civil Filings on PACER*, FULTON COUNTY DAILY REP., Dec. 18, 2002. This type of warning may have two effects: lawyers may use this information as a shield and be too cautious in briefing sensitive issues, resulting in ineffective representation; or, they may use this new device as a sword and threaten the exposure of information such as social security numbers, annual income, or even trade secrets.

[30] Lawyers, though, at all times have an ethical obligation to represent clients zealously under the rules of ethics. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 1.3 (2002) (Diligence); MODEL CODE OF PROF'L RESPONSIBILITY Cannon 7 (1983) (A Lawyer Should Represent a Client Zealously Within the Bounds of the Law).

[31] Admittedly, detailed financial information is needed in the disposition of some cases, such as divorce and bankruptcy cases. However, the publication of this information benefits society only slightly while placing litigants at a great risk of harm. While this information is necessary for the case, it should be redacted from all documents after it has outlived its usefulness in the case. The new, redacted copies should be available in both Internet and paper forms.

[32] Additionally, open access advocates urge lawyers to take advantage of the privacy safeguards already in place, such as the use of protective orders and seals on particular cases. The feasibility of this option is discussed *infra* in Section VI.A.

[33] *See* Raya Tahan, *Should Criminal Case Filings Be Available Online?*, 43 JURIMETRICS J. 43, 47 (2002) (criminal filings should be available online because the right to know, coupled with maintaining a "level playing field" for the market of court information outweighs an individual's interest in privacy).

Making public documents available online is a new convenience for those who would search the identical records in a courthouse. *See* Andrew Wolfson, *Public Access: Unlike Other States, Kentucky Keeps Online Court Records Private; Courts Weigh Convenience Against*

has the right to read, inspect, and copy documents at the courthouse, there should be no reason why those same public documents cannot be read, inspected, and copied from the Internet.[34] The ability to access government records benefits society by protecting the "integrity, quality, and respect in our judicial system."[35] Furthermore, economists and sociologists could use public information in bulk form in order to analyze human behavior.[36] Although the public does have a right to know the contents of public documents, personally identifiable information, arguably, should not be part of that public record in the first instance. Because this information is of so little value to the public and can do great harm to an individual, it should not be in public documents, and therefore, the public ought not to have a right to this information under any "right to know" ideal.

Furthermore, they state that such openness would be beneficial to the media for accurate reporting.[37] Although accuracy in the media is essential for reasons such as keeping the public informed and government accountability, these can be accomplished without making entire court documents available for public view. If a jurisdiction requires lawyers to redact particularly sensitive information—such

---

Concerns Over Privacy, THE COURIER-JOURNAL (Louisville, KY), Dec. 14, 2003, at 1A (noting that some people look through the criminal records before going out on dates, before hiring a new nanny, or before renting to tenants).

[34] *See id.* Such a right also extends from laws governing open access, such as the Freedom of Information Act (FOIA). *See* 5 U.S.C. § 552 (2000). However, the FOIA deals solely with agency rules, opinions, rulings, orders, and other information. *Id.* The legislation was never intended to serve as an "open record" law applicable to federal court documents.

[35] Video Software Dealers Ass'n v. Orion Pictures Corp., 21 F.3d 24, 26 (2nd Cir. 1994) (citing In re Analytical Sys., 83 B.R. 833, 835 (Bankr. N.D. Ga. 1987)); *see also* Peter C. Alexander & Kelly Jo Slone, *Thinking About the Private Matters in Public Documents: Bankruptcy Privacy in an Electronic Age*, 75 AM. BANKR. L.J. 437, 440 (2001) (noting that there is a constitutional presumption of open access in all civil, criminal, and bankruptcy court documents).

[36] *See* Lynn M. LoPucki, *The Politics of Research Access to Federal Court Data*, 80 TEX. L. REV. 2161, 2165 (2002). Presumably, the use of bulk data would not harm individuals so long as personally identifiable information is not being collected. Professor LoPucki noted that there might be times when the privacy concerns of an individual outweigh the research value of the material. *Id.* In these cases, she recommends that the individual take advantage of court procedures, such as sealing documents, in order to protect the privacy interest. *Id.*

[37] RAUL, *supra* note 17, at 40–41 (the media need access to public records to hold the government accountable to the citizens); FRED H. CATE & RICHARD J. VARN, THE PUBLIC RECORD: INFORMATION PRIVACY AND ACCESS—A NEW FRAMEWORK FOR FINDING THE BALANCE 11 (Coalition for Sensible Public Records 1999), *available at* http://it.ojp.gov/initiatives/files/Public_Record.pdf (last visited Jan. 22, 2003). ("Journalists rely on the public record every day to gather information and inform the public about crimes, judicial decisions, legislative proposals, government fraud, waste, and abuse, and countless other issues.")

as social security numbers—from public documents,[38] the media will still be able to report on the essential elements of a given case. Knowing such intimate personal information will not change the quality of the reporting, so redacting such information would not harm the journalism profession.

Legal research has become easier due to the increasing amount of court documents that can be accessed over the Internet. Attorneys no longer have to travel from one courthouse to another in order to collect all necessary documents. Instead, they can all be found by accessing various court websites.[39] Furthermore, copying costs are greatly minimized because a lawyer can download documents from the Internet and print them from firm printers.[40] These savings could be passed onto clients by charging reduced rates. Greater access is an undeniable benefit for lawyers and legal researchers; however, lawyers do not need to access personally identifying information, so there should be little harm if they were redacted from court records.

The risk associated with posting court documents containing sensitive information is substantial. The possibility that another will use that information to commit identity theft or to engage in discriminatory hiring or renting greatly outweighs the benefits of having personally identifying information available for the public, researchers, or the press. Furthermore, the consequences of widespread disclosure would also affect an attorney's ability to represent clients zealously and diligently. Therefore, there would be little harm in removing particularly sensitive information from generally public court documents.

III. THE EXTENT OF ELECTRONIC INVASION OF PRIVACY AT BOTH THE FEDERAL AND STATE LEVELS

Despite the need for implementing privacy legislation to protect individuals and their personally identifying information, the federal court system and most states have utilized current technology to create an even more widespread audience for this sensitive information. As technology has improved, federal and state governments have taken advantage of the advancements without first examining the existing public record laws. One of the biggest technological developments for the court systems has been the creation of electronic case management/electronic case files, or CM/ECF for short.[41] CM/ECF is a system that allows for electronic filing and management of cases, now commonly

---

[38] For a further discussion of feasibility of redacting personally identifiable information from court document, see *infra* notes 169–70 and accompanying text.

[39] *See* Rothman, *supra* note 7, at 10.

[40] *See id.* The cost of printing from a firm or personal printer is considerably less than paying for them at a copy machine at a rate of five to fifteen cents per page. However, in his article, Rothman does not acknowledge that some Internet court sites do charge users for downloading or printing the information.

[41] Askew, *supra* note 1.

referred to as e-filing.[42] This program was initiated in the federal system in 1996,[43] and the government is well underway in implementing the system nationwide.[44] The system is generally more convenient and inexpensive than traditional paper filing, so the government has embraced the new technology.[45] As a result, when the courts receive the information, it is already in digital form. The court filings can simply be accumulated into an online, searchable database.[46] CM/ECF eliminates the expensive and time-consuming process of scanning paper documents and uploading them into a database. However, older documents still must either be scanned in from the paper version or transcribed in order to be accessible online.[47] Although CM/ECF is a federal filing and management system, each state has developed some variation of this technology.[48] Some states have created their own systems, while others have

---

[42] *Id.*

[43] The federal CM/ECF service runs through a system named PACER, meaning Public Access to Court Electronic Records. PACER is the national electronic database for federal case information and is a service of the United States Judiciary, provided by the Office of the United States Court. *Clerk's Office at Your Desktop: PACER – Public Access to Court Electronic Records*, *at* http://pacer.psc.uscourts.gov/documents/pacer_brochure.pdf (last visited Jan. 22, 2004). Documents from all federal district and appellate courts received through CM/ECF are posted on PACER so attorneys can effectively monitor their cases from their computers.

[44] Askew, *supra* note 1.

[45] Gertner, *supra* note 7, at 8. To demonstrate the convenience of the system, Judge Gertner notes:

> E-filing will mean that lawyers and lay people alike will be able to file documents electronically, without leaving the office or the home. Soon the days of clutching tomes of paper and running across town to beat a filing deadline will be gone. All you need to file is a secure password and a digital signature, which are provided by the Court. With the right software, documents from any computer can be converted to a portable document format or "pdf" file and be electronically transmitted from the filer's computer system to the Court's ECF system. If you know how to use the Internet you know how to e-file. Once you sign in, you just click on a case, click on a type of motion, and append your document to the docket, and it is filed. The document is automatically updated, and the filing party receives proof of filing via email.

Id.

The use of the Internet is cost efficient and has allowed courts to reduce the size of their staff because the court websites can answer frequently asked questions, such as the hours of business and the amount of fees. Askew, *supra* note 1. Furthermore, the use of electronic filing will cut down on the number of clerks needed at the court on any given day.

[46] *See id.*

[47] See *infra* note 83 and accompanying text for a description of the costs associated with placing and maintaining an Ohio county docket online.

[48] Askew, *supra* note 1.

contracted with independent vendors.[49] Likewise, some states offer free online access, while many others charge a fee for the information.[50]

A. *Federal Databases*

Unlike many state codes, the United States Code does not have a comprehensive "public record" law.[51] In the federal system, Congress has created a piecemeal mandate for the publication of court materials through subject-specific laws and rules. For instance, agency documents are covered in one provision[52] and bankruptcy proceedings in another.[53] However, the Federal Rules of Civil Procedure require that a complete report of each and every civil case be kept by the clerk of courts.[54] These entries comprise the "civil docket."[55] Even

---

[49] *Id.*

[50] *Id.* There are two primary ways to charge a patron for use of an online database: charging for time used, or charging per page printed/downloaded. The federal database utilizes the latter of the two, charging seven cents per page with a maximum charge of $2.10 per document. *Id.* The imposition of fees could create a "digital divide" between those who can afford to pay for the documents and those who cannot. This issue should be considered whenever a jurisdiction contemplates implementing a fee structure.

[51] *Contra* OHIO REV. CODE ANN. § 149.011(G) (Anderson 2001) ("'Record' includes any document . . . created or received or by coming under the jurisdiction of any public office of the state or its political subdivisions which, serves to document the . . . decisions . . . of the office."); OHIO REV. CODE ANN. § 149.43 (Anderson 2002) (broadly defining "record" and then allowing specific exceptions, such as medical records and attorney work product materials).

[52] *See* 5 U.S.C. § 552a(b)(11) & (e)(8) (2000) (agency records on an individual are generally not public records unless they are discovered pursuant to a court order and then placed in the public record of a lawsuit). The agency records covered under this code provision are those that the agency gathers on regulated individuals. It does not include records that are part of either agency rulemaking or adjudication. Many agencies do publish documents in association with these functions online. See *supra* note 2 for examples of agencies that publish adjudicative rulings on their websites.

[53] *See* FED. R. BANKR. 2013 (the clerk shall maintain a record of all of the fees awarded in each bankruptcy, and the record will list the docket number, the name of the case, and the amount awarded to each creditor); FED. R. BANKR. 2015 (Chapter 11 financial reports prepared by the bankrupt may be published by order of the court.).

[54] FED. R. CIV. P. 79. This rule reads, in pertinent part:

> The clerk shall keep a book known as "civil docket" . . . and shall enter therein each civil action to which these rules are made applicable. Actions shall be assigned consecutive file numbers. . . . All papers filed with the clerk, all process issued and returns made thereon, all appearances, orders, verdicts, and judgments shall be entered chronologically in the civil docket on the folio assigned to the action and shall be marked with its file number. These entries shall be brief but shall show the nature of each paper filed or writ issued and the substance of each order or judgment of the court and of the returns showing execution of process.

though the Rules do not specifically mention that the civil docket becomes part of the public record, Rule 79 mandates that the courts keep records in a systematic manner to be used later by courts of appeals and to be open to the public.

The public record is primarily viewed online through the federally sponsored PACER system.[56] It is a service of the United States Judiciary and is run by the Administrative Office of the United States Courts.[57] PACER offers its users a plethora of information on federal cases, including the parties and judge in a case, docket entries, judgments, and even imaged copies of documents.[58] There is a comprehensive "U.S. Party/Case Index" that is a searchable database for all

---

FED. R. CIV. P. 79(a). The civil docket includes every document that is either generated by the court or that passes through the court. The only documents that are not included as part of the docket are discovery requests that are given directly from one attorney to another without the assistance of the court. Of course, if the judge rules on a discovery matter, that will be part of the official record.

[55] *Id.*

[56] PACER can be found on the Internet at www.pacer.psc.uscourts.gov (last visited Jan. 22, 2004). Note that many private vendors also offer online docket services. CourtEXPRESS is the leading private vendor offering users the ability to run searches offline and saving multiple searches. The cost of using this network begins at $69 per case and $8 per docket page accessed. *See* http://www.courtexpress.com/index.cfm?action=priceinfo (last visited Mar. 10, 2004). LexisNexis offers the service CourtLink that allows subscribers to search with detailed guided search forms and to receive e-mail case updates. CourtLink charges $5 per case retrieved, plus charges for viewing the case and printing it. *See* http://www.lexisnexis.com/courtlink/online (last visited Jan. 22, 2004).

[57] http://pacer.psc.uscourts.gov/faq.html#CR7 (last visited Jan. 22, 2004). There are two ways to access PACER. The first, and most convenient, is through the Internet, at http://www.pacer.psc.uscourts.gov. However, for those who do not have a regular Internet provider, the government offers access to the system via dial-up connection. Due to these different methods of access, the government designed two ways in which to charge its users for using the service. For those who access PACER by the Internet, the government charges seven cents per page downloaded with a maximum charge of $2.10 per document not exceeding thirty pages. *Clerk's Office at Your Desktop: PACER – Public Access to Court Electronic Records*, *available at* http://pacer.psc.uscourts.gov/documents/pacer_brochure.pdf (last visited Jan. 22, 2003). Those who use the dial-up service are charged sixty cents per minute, without regard to the number of documents downloaded or printed in the amount of time spent online. *Id.* Registered individuals are billed quarterly, but only if their current charges total more than ten dollars. http://pacer.psc.uscourts.gov/faq.html#CR7 (last visited Jan. 22, 2004). Detailed account histories can be viewed online, and individuals can assign client numbers to particular searches in order for individuals to pass the expenses onto their clients. *Id.*

[58] http://pacer.psc.uscourts.gov/pacerdesc.html (last visited Oct. 20, 2003). PACER also allows users to search for the following information: parties and participants in a case including judges, attorneys, and trustees; case-related information such as cause of action, nature of suit, and damages; a chronology of case events entered into the record; a claims registry; a list of each day's new cases; appellate opinions; judgments or case status; various types of documents filed for some cases, such as motions and briefs; and imaged copies of documents. *Id.*

federal cases that have online access.[59] To search the bankruptcy index, the user must provide an individual's name or social security number; to locate a civil case, the user must provide only the name of a party or the nature of the suit;[60] to look up a criminal record, the user need only provide the name of the defendant; and, to search for an appellate review of a case, only the name of the party is necessary.[61] After entering a search term, "[e]ach hit produced from your searches will give you the party name, the court where the case is filed, the case number, and the filing date. In addition, for bankruptcy searches you will receive the chapter, and for civil searches you will receive the nature of suit."[62] If the searcher wants more information on the case, he or she can dial directly into the particular jurisdiction's PACER system to see if that jurisdiction offers other documents online, such as lawyer's motions or briefs, or any court ruling.[63]

The most significant shortcoming of the PACER system is the inconsistency with which records are made available.[64] Although the website is managed by the Administrative Office of the United States Courts, the federal government allows each district discretion to choose the materials it will place online.[65] Each federal court determines what documents, if any, will be available for online viewing.[66] These documents will either have to be scanned into the system or received by the court through online filing. Although PACER allows a system user to download

---

[59] The Judiciary has created the U.S. Party/Case Index due to the increased demand for judicial materials. The largest push for such a comprehensive service came from "organizations tracking regional or national bankruptcy, civil or criminal litigation [who] have requested more efficient methods to retrieve case information from multiple court jurisdictions." http://pacer.psc.uscourts.gov/uspci.html (last visited Jan. 22, 2004).

[60] There is a code system to define the nature of the civil actions. Each classification of civil action is given a three-digit code number, with the first digit of the code denoting the broadest category of a suit. For example, the 100 series deals with contracts, the 300 series deals with torts, and the 400 series with civil rights. http://pacer.psc.uscourts.gov/natsuit.html (last visited Jan. 22, 2004).

[61] *See* http://pacer.psc.uscourts.gov/uspci.html (last visited Jan. 22, 2004).

[62] *Id.*

[63] *Id.*

[64] There are two distinct types of inconsistencies. First, jurisdictions are inconsistent in determining whether or not they will place any documents on the Internet. Currently, only six district courts, six bankruptcy courts, and five appellate courts are not connected to PACER in any manner. *See* http://pacer.psc.uscourts.gov/cgi-bin/miss-court.pl (last visited Jan. 22, 2004). And second, among those jurisdictions that do place documents online, not every jurisdiction makes available the same types of documents. For instance, not every jurisdiction places attorney briefs online.

[65] http://pacer.psc.uscourts.gov/faq.html#CR7 (last visited Jan. 22, 2004).

[66] *See id.*; *see also* Rothman, *supra* note 7, at 10. Rothman notes, "[a]t present, the courts have no uniform policy in place regarding public access to electronic court records. Clerks have been guided by decisions around the country that have found a strong presumption, but not an absolute right, in favor of public access to all documents filed in court." *Id.*

documents already placed online, it does not guarantee that any district will have particular documents available.[67] The disparity of online access could result in forum shopping because lawyers may be more inclined to file in a district that does—or does not—publish its record online to protect the privacy of the clients.

B. *Selected State Laws that Pose Particular Threats to Privacy*

Unlike the federal government, each state has enacted open access statutes defining public records.[68] Under these statutes, many states have started to post their public judicial documents on the Internet. Generally, states do not sponsor the court websites, but they allow individual districts to place their own documents online.[69] Greater autonomy for individual districts, however, leads to greater disparity of electronic information. This section will examine the laws of Ohio, Florida, and Maryland—three states that are leading the way towards greater online availability of resources.

1. *Ohio*

In Ohio, the Public Records Act is broad, paving the way for districts to place public court documents on the Internet. The Ohio act begins with a blanket

---

[67] *See* http://pacer.psc.uscourts.gov/faq.html#CR7 (last visited Jan. 22, 2004).

[68] ALA. CODE § 36-12-40 (2002); ALASKA STAT. § 40.25.110 (Michie 2002); ARIZ. REV. STAT. § 39-121.01 (2002); ARK. CODE ANN. § 25-19-105 (Michie 2002); CAL GOV'T CODE § 6252 (West 2002); COLO. REV. STAT. § 24-72-303 (2002); CONN. GEN. STAT. § 1-200 (2002); DEL. CODE ANN. tit. 29, § 10002 (2002); D.C. CODE ANN. § 2-502 (2002); FLA. STAT. § 119.01 (West 2003); GA. CODE ANN. § 50-18-70 (2002); HAW. REV. STAT. § 92F-3 (2002); IDAHO CODE § 9-337 (Michie 2002); 5 ILL. COMP. STAT. § 140/2 (2002); IND. CODE § 5-14-3-2 (2002); IOWA CODE § 22.1 (2002); KAN. STAT. ANN. § 45-217 (2002); KY. REV. STAT. ANN § 61.870 (Michie 2002); LA. REV. STAT. ANN. § 44:1 (West 2002); ME. REV. STAT. ANN. tit 1, § 402 (West 2002); MD. CODE ANN., STATE GOV'T § 10-611 (2002); MASS. GEN. LAWS ch. 66, § 1 (2002); MICH. COMP. LAWS § 15.232 (2002); MINN. STAT. § 13.01 (2002); MISS. CODE ANN. § 25-61-3 (2002); MO. REV. STAT. § 109.210 (2002); MONT. CODE ANN. § 2-6-101 (2002); NEB. REV. STAT. § 84-712 (2002); NEV. REV. STAT. § 239.010 (2002); N.H. REV. STAT. ANN. § 91-A:1 (2002); N.J. STAT. ANN. § 47:1A-1 (West 2002); N.M. STAT. ANN. § 14-3-2 (Michie 2002); N.Y. PUB. OFF. LAW § 87 (McKinney 2002); N.C. GEN. STAT. § 132-1 (2002); N.D. CENT. CODE § 44-04-18 (2002); OHIO REV. CODE ANN. § 149.43 (West 2002); OKLA. STAT. tit. 51, § 24A.3 (2002); OR. REV. STAT. § 192.001 (2002); PA. STAT. ANN. tit. 65, § 66.1 (West 2002); 32 P.R. LAWS ANN. § 1781 (2002); R.I. GEN. LAWS § 38-2-2 (2002); S.C. CODE ANN. § 30-4-20 (Law. Co-op. 2002); S.D. CODIFIED LAWS § 1-27-21 (Michie 2002); TENN. CODE ANN. § 10-7-503 (2002); TEX. GOV'T. CODE. ANN. 552.022 (Vernon 2002); UTAH CODE ANN. § 63-2-201 (2002); VT. STAT. ANN. tit. 1, § 317 (2002); VA. CODE ANN. § 2.2-3701 (Michie 2002); 3 V.I. CODE ANN. § 881 (2002); WASH. REV. CODE § 42.17.250 (2002); W. VA. CODE § 29B-1-1 (2002); WIS. STAT. § 19.35(1) (2002); WYO. STAT. ANN. § 16-4-201 (Michie 2002).

[69] *See supra* notes 48–50 and accompanying text.

statement declaring that government records are public.[70] Only after this blanket statement does the statute provide any exceptions.[71] The statute allows for twenty-two exceptions, including exceptions for medical records, information contained in the putative father registry, trial preparation materials, and DNA records.[72] Court documents, ranging from docket entries to lawyers' briefs, to court opinions, are public records because they are "records kept by any public office."[73]

The Ohio Supreme Court has repeatedly stated that the Public Record Act should be interpreted broadly. The Court offers two reasons for this interpretation. First, access to public records is a policy favored in society; and therefore, borderline questions should be determined in favor of greater access.[74] Secondly, as a matter of statutory construction, exceptions to a general rule should be construed narrowly, especially if the rule contains many narrowly drawn exceptions.[75]

Hamilton County, Ohio[76] has placed its entire docket and many of its past docket entries online.[77] The website is searchable, and the site user need only pick

---

[70] OHIO REV. CODE ANN. § 149.43 (West 2002). The law states:

> "Public record" means records kept by any public office, including, but not limited to, state, county, city, village, township, and school district units, and records pertaining to the delivery of educational services by an alternative school in Ohio kept by a nonprofit or for profit entity operating such alternative school pursuant to section 3313.533 of the Revised Code.

OHIO REV. CODE ANN. § 149.43(A)(1) (West 2002).

[71] *Id.* (At the end of subsection (A)(1), the statute reads, " '[p]ublic record' does not mean any of the following:")

[72] *Id.* There is no final, catch-all provision in the Ohio statutes. Thus, the only exceptions are those enumerated. Currently, there is no exception for court records of any type.

[73] *Id.*

[74] *See, e.g.*, State *ex rel.* Consumer News Serv., Inc. v. Worthington City Bd. of Educ., 776 N.E.2d 82, 88 (Ohio 2002) ("[W]e must liberally construe [the public record act] in favor of broad access and resolve any doubt in favor of disclosure of public records."); State *ex rel.* Thomas v. Ohio State Univ., 643 N.E.2d 126, 128 (Ohio 1994) (Ohio Revised Code § 149.43 "generally is construed liberally in favor of broad access, and any doubt must be resolved in favor of disclosure of public records.").

[75] *See, e.g.*, State *ex rel.* King v. Wachenschwanz, 757 N.E.2d 367, 370 (Ohio 2001) ("Exemptions from disclosure must be strictly construed against the public records custodian, and the custodian has the burden to establish an exemption.").

[76] Hamilton County is the home of Cincinnati, Ohio.

[77] The Hamilton County Clerk of Courts Website can be accessed at http://www.courtclerk.org (last visited Jan. 16, 2003). Currently, the Hamilton County Website is free of charge and open to anyone with Internet access. System users need not create passwords or provide the county with personal information to use the resources. The county does not charge users for either downloading information or for printing. However, because there are no "log-on" procedures, the system does not keep track of an individual's past

a name to proceed.[78] The "Comprehensive Name Index to Cases" allows a system user to search "Common Pleas and Municipal, civil and criminal cases, judgments, and tickets (citations) all" at once.[79] The "Case Inquiry" screen allows a user to choose to search different divisions of the record, such as Common Pleas Civil, Criminal, and Municipal Civil, for a less extensive search.[80] By clicking on a docket entry, the website will give the system user the names of the parties involved in the action, the type of action, the nature of the lawsuit, the case number, the date of filing, court costs, and the amount of money currently filed with the court.[81] Hamilton County has, by far, the most extensive court website in Ohio.[82]

To maintain a website, each county must invest money to scan documents into ".pdf" form and to maintain a searchable database. Not every county has the resources to do this. For instance, Sandusky County has experienced budget

---

searches, and it is hard to navigate through a search without continually re-transmitting the search terms.

[78] The Website user could choose to look up either someone the user knows or a complete stranger. Simply searching common last names, such as Smith or Jones, brings up hundreds of results.

[79] http://www.courtclerk.org (last visited Jan. 16, 2003). In order to search the Comprehensive Name Index, the system user must enter a last name and at least the first letter of an individual's name, or a company's name. If the computer does not find any matches, it will search nearby letters.

[80] http://www.courtclerk.org/cas_rpt.htm (last visited Jan. 16, 2004). Within each of these divisions, one can search under the name index, the case docket number, or attorney. When the website is searching for a particular name or number, the results retrieved will include both "direct hits" and near misses.

[81] A simple search for my last name led me to one exact hit and three near misses in the Common Pleas Civil docket. Clicking on any one of these entries led me to the screen with all of the basic information just described.

[82] Cuyahoga County, home of Cleveland, Ohio, also has an online docket for both criminal and civil cases. *See* http://www.cuyahoga.oh.us/common/default.htm (last visited Jan. 16, 2004). The online criminal docket is searchable by defendant's name or case number. A name search must include a last name and at least two letters of a first name. Each "hit" lists the defendant's name, date of birth, race, and gender. Then, the database user can click onto an individual case to learn of the charges, the pleas, and the sentence. Plus, there is a summary of each instance that the defendant appeared before the court in any particular case under the label "Case Notes." *See* http://cpdock.cuyahoga.oh.us/cpdock/ (last visited Jan. 16, 2004). The civil docket is also searchable by name or case number. A name search on the civil docket only requires two letters in a party's last name. Each "hit" lists the case number and the address of the litigant. Clicking on an entry will allow the user to discover the type of dispute, the method of process used, and the costs associated with the claim. There is also a feature that displays all of the docket entries. There is a list of links to imaged copies of court filings; however, few documents are actually available online. *See* http://cpdocket.cuyahoga.oh.us/cjisjs/servlet/cjis.urd/run/cmsw101 (last visited Jan. 16, 2004).

problems that prohibit the clerk from creating an online database.[83] The budget cuts have even forced the layoffs of individuals responsible for converting paper documents into electronic form, resulting in further delays.[84]

As a result of Hamilton County's extensive website, the former Hamilton County Clerk of Courts James C. Cissell proposed state legislation that would better protect Ohio's citizens.[85] The proposed rules would create uniform rules for sealing documents and then urge the use of filing documents containing sensitive information under seal.[86] This approach does not forbid the use of personally identifying information, but rather broadens the use of the judicial protection of documents. Under this model, the initial burden of preserving privacy rests on the attorney to seek seal, but the judge ultimately decides what information should be private. Although this is a more flexible approach than requiring redaction of categories of information, this model places a tremendous burden on the courts to seal records and it creates judicial discretion in determining what information should be confidential.

---

[83] Yena Peach Hart, *Online Effort Off Line for Clerk of Courts*, THE NEWS-MESSENGER, December 10, 2002, at 1A. The project would cost the county approximately $13,000 to initially place the documents online, plus $ 1,000 per month to maintain the website. *Id.*

[84] *Id.* Sandusky County Clerk of Courts Warren Brown lamented that,

> Everything hinges on the budget and the position of the Supreme Court on the matter of what is truly a public record—where do you draw the line between what is a public document and what is a person's private life .... I would love to be able to put some of these records online. For now, it's as far back on the burner as you can push it, but the fire is not completely out.

Id.

[85] The website used to contain a link to a ".pdf" version of the proposed model Ohio rules. However, after a new County Clerk of Courts was elected in November 2002, this link was removed.

[86] James C. Cissell, *Proposal to Protect Sensitive Personal Information in Ohio Public Records* 2, *available at* http://www.courtclerk.org/images/statuteamendments.pdf (last visited Jan. 16, 2004). The proposal also urges that any documents sealed at the lower court should be remained sealed on appeal. *Id.* Documents that would commonly qualify for sealing include social security numbers required in divorce actions, other documents with social security numbers, and documents containing financial, mental health, family relation, or medical information in a domestic relations case. *Id.*

One judge in neighboring Butler County has taken a more extreme action to protect the privacy of those before the domestic relations court. As of July 1, 2003, Judge Leslie Spillane ordered that all domestic relations documents be removed from the Internet. Judge Leslie Spillane, *Internet Access to DR Case Information*, July 7, 2003, *at* http://www.butlercountyohio.org/drcourt/pdfs/Internet%20Access.pdf (last visited Jan. 16, 2004); *see also* Hudak, *supra* note 25, at B1 (quoting Judge Spillane stating that neighbors and other nosey people do not have the right to poke into the problems of divorcing couples in order to uncover some "dirt").

2. *Florida*

Like Ohio, Florida has made great strides toward allowing, and even mandating, counties to place court dockets online. Florida, too, has a blanket "open record" statute.[87] The statute even accommodates for the changing use of technology.[88] It provides:

> The Legislature finds that, given advancements in technology, providing access to public records by remote electronic means is an additional method of access that agencies should strive to provide to the extent feasible. If an agency provides access to public records by remote electronic means, then such access should be provided in the most cost-effective and efficient manner available to the agency providing the information.[89]

Furthermore, the statutes mandate that each county maintain an online docket by the year 2006.[90] Certain records, though, are exempted from Internet dissemination. These records include images or copies of military discharges, death certificates, and any materials in cases governed by the Florida Rules of Family Law, the Florida Rules of Juvenile Procedure, or the Florida Probate Rules.[91]

In an advisory opinion, the Florida Supreme Court upheld these statutes.[92] The court recognized the need to balance the rights of all individuals to have access to public documents and the need for privacy for the individuals mentioned in the documents.[93] The court is concerned that confidential, yet

---

[87] FLA. STAT. ANN. § 119.01(1) (West 2002). ("[I]t is the policy of this state that all state, county, and municipal records shall be open for personal inspection by any person.").

[88] *See* FLA. STAT. ANN. § 119.01(2) (West 2002).

[89] *Id.*

[90] FLA. STAT. ANN. § 28.2221(5)(e) (West 2002). At a minimum, each county must provide remote electronic access to "images of documents referenced as the index required to be maintained on the county's official records website by this section." *Id.* At this time, there are some Florida districts that do not even have a website. It seems highly unlikely that these districts will be able to coordinate websites with searchable databases by 2006.

[91] FLA. STAT. ANN. § 28.2221(5)(a) (West 2002).

[92] *See In re* Report and Recommendations of the Judicial Management Council of Florida on Privacy and Electronic Access to Court Records, 832 So. 2d 712 (Fla. 2002). *See also* CAL. R. CT. 2070–2077 (2002). California, by Rule, excepted certain types of documents from Internet dissemination, including records from juvenile court, guardianship or conservatorship proceedings, mental health records, criminal records, and any documents from any proceedings under the Family Code and the Code of Civil Procedure § 527.6 relating to civil harassment. *See* Carole Levitt, *Regulating the Availability of Public Records Online: Federal and State Courts are Working to Balance Issues of Privacy and Public Access*, L.A. LAW., Dec. 2002, at 38. These California rules took effect July 1, 2002 and were promulgated to address privacy concerns. *Id.*

[93] *See In re* Report on Privacy, 832 So. 2d at 712–13.

discoverable, information may be transformed into public information if it is placed in an attorney's brief.[94] Furthermore, court records often contain information that is not technically "confidential," but is still sensitive.[95] However, the court held that the problem requires a legislative, not judicial, solution.[96] The court expressed satisfaction with the current limitations on the open record laws, especially the "temporary limited moratorium" on obtaining access to military discharges, death certificates, and case material from family law, juvenile law, and probate law cases.[97]

Some Florida counties are already in compliance with the requirements for online dockets. For instance, Lake County has maintained an online database for nearly a year and a half.[98] The site is searchable by name, document type, docket number, or even by book and page number.[99] There are further field restrictors, such as date and a limitation on the number of documents retrieved.[100] When the search results are returned, each hit contains the names of the parties, the docket number, the date filed, and various codes denoting the case status and type.[101] By clicking on any entry, the next screen will allow a user to see images of the final judgments of cases.[102] Searching the database is free of charge, but the images retrieved are not certified copies.[103] However, a system user can link to www.myflorida.com to order certified copies of the same documents at a charge

---

[94] *Id.* at 714.

[95] *Id.*

[96] *Id.* at 715 ("While no party disputes that this Court has a rule in formulating statewide policies on access to Court records, we are also mindful of the Legislature's parallel initiative in forming and funding a study committee, including members of the judiciary, to specifically examine electronic access to court records. Thus it appears that any effort proposed by the Council on this Court's behalf would likely be redundant to the Legislature's Study Committee on Public Records.").

[97] *Id.*

[98] Owens, *supra* note 7, at G3.

[99] *See* http://www.lakecountyclerk.org (last visited Jan. 16, 2003). To search for an individual, one must know his or her last name. Entering a fist name is optional. Business entities can also be searched by the name of the corporation.

[100] *Id.* There are also other helpful options, such as limiting a search by date and formatting the number of documents the user wishes to view on a page at a single time.

[101] *Id.*

[102] *Id.*

[103] *See* http://lakecountyclerk.org/services.asp?subject=Online_Court_Records (last visited Jan. 16, 2004). Upon entering the website, there is a disclaimer stating that the user understands that the documents presented online are not certified. A user can only access the court documents upon clicking "I Agree" to the disclaimer.

of one dollar per page with additional fees for online transactions.[104] However, a person must become a registered subscriber in order to access this material.[105]

As a result of these aggressive requirements, Chief Justice Harry Lee Anstead of the Florida Supreme Court declared a temporary moratorium on placing court documents on the Internet.[106] The purpose of the moratorium is to determine if the legislation ordering online dissemination protects adequately protects the privacy rights of individuals.[107] The moratorium will only affect court documents, and it will not affect the availability of other information, such as court dockets and calendars.[108] The ban on Internet dissemination of court documents will be in place at least until July 1, 2005 when a panel of fifteen experts must submit guidelines to the court.[109]

3. *Maryland*

Maryland's statutory scheme regarding public records is quite extensive.[110] The language of the Maryland Public Information Act, at first, is all encompassing;[111] however, the scope is immediately restricted in the next

---

[104] *See* http://www.myfloridacounty.com (last visited Jan. 16, 2004). Myfloridacounty.com also maintains a comprehensive list of all of the counties that are currently online.

[105] *See* http://www.myfloridacounty.com/services/officialrecords_intro.shtml (last visited Jan. 16, 2004).

[106] *See* Jim Ash, *Curbs on Online Court Records Foster Confusion*, PALM BEACH POST, Dec. 13, 2003, at 1A; Laurie Cunningham, *Top Judge Freezes Web Postings; He Fears Dissemination of Sensitive Online Data*, AM. LAW. MEDIA NEWS SERVICE, Dec. 8, 2003, at 5.

[107] Ash, *supra* note 106, at 1A.

[108] *Id.* ("[P]eople will still have Internet access to court calendars and dockets that track the progress of cases as well as lists of judgments, court orders, pleadings and motions.").

[109] *Id.*

[110] *See* MD. CODE ANN., STATE GOV'T §§ 10-601–642 (1999 & Supp. 2002). Like Ohio and Florida, the Maryland code begins with a broad statement of what constitutes an open record; however, the Maryland statutes explicitly limit the openness of certain records. The Code categorically limits access to certain types of records largely relating to family and other personal records. MD. CODE ANN., STATE GOV'T § 10-616 (2002). Examples of records with limited access include adoption records, welfare records, hospital records, and certain school and transportation records. *Id.*

[111] MD. CODE ANN., STATE GOV'T § 10-612 (2002). The statute begins with a general statement of public access: "All persons are entitled to have access to information about the affairs of the government and the official acts of public officials and employees." MD. CODE ANN., STATE GOV'T § 10-612(a) (2002). Although this section of the act does not mention the court system, records produced by the court system are clearly covered because members of the judiciary are "court officials." Furthermore, the statute defines a "public record" to be one made by "a unit or instrumentality of the State government or of a political subdivision or received by the unit or instrumentality in connection with the transaction of public business." MD. CODE

subsection.[112] By definition, rather than by court interpretation, records of all types, including electronic records, fall within the meaning of "public record."[113] The code specifically differentiates between "public records"[114] and "personal records."[115] Maryland law, then, takes an extraordinary step and sets forth a limited right to privacy when the dissemination of public documents is an "unwarranted invasion" of privacy.[116] This right to privacy, though, is limited

---

ANN., STATE GOV'T § 10-611(g)(1)(i) (2002). Documents created by the court, such as docket information, rulings on motions, and court opinions would fall within the category of a record made by an instrumentality of the government; likewise, materials prepared by lawyers, such as motions, memoranda, and briefs would fall within the latter half of the definition covering materials received by the government in connection with public business. *See id.*

[112] Immediately following the expansive language of subsection (a), the legislature limited the scope of the act in subsection (b) by noting that "the right set forth in subsection (a) of this section [would be carried out], unless an unwarranted *invasion of privacy* of a person in interest would result . . . ." MD. CODE ANN., STATE GOV'T § 10-612(b) (2002) (emphasis added).

[113] MD. CODE ANN., STATE GOV'T § 10-611(g)(1)(ii)(2) (2002). The express language reaches "a computerized record," and records that are maintained both online and in a central courts' web server are likely to be classified as "computerized" records. The statute attempts to reach all forms of records, including cards, letters, drawings, films, microfilms, forms, maps, photographs, recordings, and tapes. MD. CODE ANN., STATE GOV'T § 10-611(g)(1)(ii) (2002). Although the statute enumerates certain types of records, the list is not intended to be exhaustive, but to be able to accommodate for new technologies and innovations. *Id.* (A public record is a record in "any form, including . . . .").

[114] *See* MD. CODE ANN., STATE GOV'T § 10-611(g) (2002).

[115] MD. CODE ANN., STATE GOV'T § 10-611(f) (2002). "Personal information" is defined as "information that identifies an individual [sic] including an individual's address, driver's license number or any other identification number, medical or disability information, name, photograph or computer generated image, Social Security number, or telephone number." MD. CODE ANN., STATE GOV'T § 10-611(f)(1) (2002). Specifically excluded from this definition is information pertaining to a person's "driver's status, driving offenses, 5-digit zip code, or information on vehicular accidents." MD. CODE ANN., STATE GOV'T § 10-611(f)(2) (2002). It is unclear from the definition whether a personal record must be entirely personal or if certain portions of a generally public document are also deemed as personal if they contain personally identifying information. Almost all court documents would fall within this seemingly intermediate category because these documents, admittedly public records, do contain an individual's name, address, and sometimes even a social security number; however, the records were not created merely to store personal information on the party.

[116] MD. CODE ANN., STATE GOV'T § 10-612(b) (2002). The pertinent section of the code states:

> To carry out the right set forth in subsection (a) of this section, *unless an unwarranted invasion of the privacy of a person in interest would result*, Part III of this subtitle shall be construed in favor of permitting inspection of a public record, with the least cost and least delay to the person or governmental unit that requests the inspection.

Id. (emphasis added).

because of the general policy in favor of open access.[117] Thus, the law presumes that the government records are open, but that there are instances in which the invasion of privacy is so egregious that dissemination would be deemed an "unwarranted invasion" of an individual's privacy.

The courts have generally interpreted the Maryland Public Information Act liberally to allow for disclosure in most cases.[118] Furthermore, the information must fall within a specifically enumerated exception to be held as private.[119] In 1998, the Maryland Supreme Court addressed the issue of an "unwarranted invasion" of another's privacy in *Kirwan v. The Diamondback*.[120] The court noted that this limiting language appeared in the section defining the statute's general scope, and because the scope of the Act is broad, the limitation should be narrowly construed.[121] In its analysis, the court acknowledged that the language existed;[122] however, it appeared to require that the information fall within an exemption to be considered an unwarranted invasion of privacy.[123] By limiting

---

[117] *Id.* In this regard, Maryland acts in a similar manner as both Ohio and Florida, both of which strongly favor the dissemination of public records. *See* State *ex rel.* Consumer News Serv., Inc. v. Worthington City Bd. of Educ., 776 N.E.2d 82, 88 (Ohio 2002); State *ex rel.* Thomas v. Ohio State University, 643 N.E.2d 126, 128 (Ohio 1994); State *ex rel.* King v. Wachenschwanz, 757 N.E.2d 367, 370 (Ohio 2001); *see also* FLA. STAT. ANN. § 119.01(2) (West 2002).

[118] *See, e.g.*, Office of Attorney General v. Gallagher, 753 A.2d 1036, 1037 (Md. 2000) ("In order to carry out this right of access, the Act is to be construed in favor of disclosure."); Kirwan v. The Diamondback, 721 A.2d 196, 203 (Md. 1988) (The scope of the Maryland Public Information Act is broad as a matter of statutory interpretation and public policy.); Bowen v. Davidson, 761 A.2d. 1013, 1016 (Md. App. 2000) ("The Act must be construed liberally in favor of disclosure.").

[119] *See, e.g.*, Kirwan v. The Diamondback, 721 A.2d 196, 203 (Md. 1998) (exceptions to the Public Information Act should be construed narrowly); Bowen v. Davidson, 761 A.2d 1013, 1016 (Md. App. 2000).

[120] 721 A.2d 196, 203 (Md. 1998). This case dealt with the investigation by the school newspaper of preferential treatment of men's basketball players. Allegedly, the coaching staff would pay for parking tickets received by the players when they would park illegally in handicapped spots. *Id.* at 198. The newspaper sought the university records stating who had paid the fines, and the university refused on the grounds that the information was confidential under either the exemption for education personnel records or the exemption for financial records. *Id.* at 198–99.

[121] *Id.* at 203.

[122] *Id.* ("assuming *arguendo* that one might reasonably believe that such disclosure is an unwarranted invasion of privacy . . .").

[123] *Id.* The relevant language of the court is as follows: "[t]he Maryland Public Information Act does not contain an exception for particular cases whenever the disclosure of a record might cause an 'unwarranted invasion of privacy.'" *Id. But see* Young v. State, 806 A.2d 233, 252 n.13 (Md. 2002). In this case dealing with the publication of sex offender registries, the court upheld the publication, but mentioned in a footnote that:

the exemption to information already covered in the Act, the court turns the exception into mere surplusage. To date, no case has relied on the "unwarranted invasion of privacy" language to prohibit disclosure of otherwise public information.[124] Perhaps a challenge to court documents placed on the Internet that contain social security numbers or other personal identification would be considered an "unwarranted invasion of privacy," but this issue has not yet been tested.

Currently, access to Maryland court information available online is significantly more limited than in Ohio and Florida. The central Maryland webpage[125] allows dial-up access to its database; however, those interested in obtaining access must first complete a "Public Access and Inquiry Request Form and Disclaimer Form"[126] and pay a fee.[127] The information online comes from a variety of different sources,[128] but is limited to what individual courts decide to

---

> It is arguable that widespread Internet community notification stigmatizes registrants and implicates liberty and privacy interests that would satisfy the "stigma plus" test utilized to analyze civil due process challenges in many of the federal circuits, therefore requiring certain procedural due process protections beyond those provided in the statute prior to notification.

Id. Although this footnote states that the registries are constitutional, whether in paper or electronic form, the court recognizes that Internet dissemination of information raises interesting questions of balancing privacy and public access.

[124] Note, however, that cases are still heard regarding the enumerated exceptions to the Maryland Public Information Act found in sections 10-615 through 10-619. Yet, because the exceptions are strewn so narrowly, it is extremely difficult for a party to convince the court that information falls within these categories. As stated, *supra* note 111, court documents probably do not fall within any of the exceptions, and thus a court is likely to find that court documents are public information that can be disseminated over the Internet, even if they contain personal identifying information.

[125] *See Dial Up Access to Maryland Court Sytems*, at http://www.courts.state.md.us/dialup.html (last modified Feb. 10, 2004). The only access to the court records is through the dial-up system. The state does not have an Internet/DSL database at this time.

[126] *Id.* The state requires certain information from each of its applicants, including a billing name and address, e-mail address, and social security or federal tax identification number. *See* http://www.courts.state.md.us/signupin.pdf (last visited Mar. 10, 2004). By asking for the company name and address, rather than an individual's name and address, the courts clearly are aiming at attracting businesses and law firms.

[127] *Dial Up Access to Maryland Court Systems*, *at* http://www.courts.state.md.us/dialup.html (last visited Mar. 10, 2004). There is a fee of fifty dollars that is pro-rated at twenty-five dollars for the first six months of the year. The use of fees can, at times, deter a "bad actor" from pursuing his or her course of criminal action. However, whether fifty dollars is a sufficient deterrent is unclear. The purpose of the fee, too, is not mentioned; the fee could be used both for a deterrent effect and to fund the maintenance of the web server.

[128] *Id.* The court systems that can be accessed include the Maryland District Court, the Uniform Civil Court (Circuit Court Civil), the Circuit Court Land Plat Automated Indexing System, the Circuit Court Civil case management system, the Circuit Court Criminal/Paternity

place online. Furthermore, the databases are searchable *only* by party name or case number,[129] making it harder for a user to search generally.[130]

The judiciary formed a committee to study the current access to Maryland court documents and to assess the proper course of future action.[131] The committee noted that the state currently adequately protects the privacy of its citizens;[132] however, it realizes that the increasing use of electronic access might eventually jeopardize personal privacy.[133] The report begins with a general and dynamic definition of "court records" that includes electronic documents.[134] After

---

and Non Support for Baltimore City, and the Ann Arundel and Carroll County Circuit Court systems. *Id.* The website notes that the records from any individual court are incomplete, and it further warns users that the only documents that have been filed with a court in connection with a particular case that might be available online are not confidential or protected by a court order. *Id.*

[129] *Id.*

[130] For instance, if a person with "bad intent" were to register with the state to use the database and pay the fifty-dollar fee, he or she would *also* have to know their victims ahead of time. If the person were searching for a credit card number, that person would also have to know that the victim recently filed papers with the court that would contain this information.

[131] *See* Hon. Paul E. Alpert, et al., *Report of the Committee on Access to Court Records* 1, *available at* http://courts.state.md.us/access/finalreport3-02.pdf (last visited Mar. 10, 2004). Included among the seventeen committee members were four other judges, Hon. Joseph M. Getty, Hon. Sharon M. Grosfeld, Hon. Patrick J. Hogan, and Hon. Philip C. Jimeno, and at least five lawyers.

[132] *See id.* at 4. The files that are available in electronic form are limited in nature. Furthermore, these files can only be accessed by four methods: use of computers located at the courthouse for public use, remote "dial up" access subject to registration, remote access to data via modem pursuant to an agreement with the court, and access to data compilations also pursuant to an agreement with the court. *Id.*

[133] *Id.* at 1 ("In light of . . . concerns, traditional access policies need to be reconsidered, in order to insure that the proper balance is maintained between public access, public safety, privacy, and risk of harm while maintaining the integrity of the judicial process.").

[134] *Id.* at 2. The committee defines court records as:

> (a) documents, information or other things that are collected, received or maintained by a court in connection with a court case; and (b) indexes, calendars, orders, judgments or other documents and any information in a case management system created by the court that is related to a court case. The physical form of court records may be paper, electronic, or other.

Id. The definition explicitly excludes records not maintained in connection with a case, judge's notes and other work product, and agency information to which the court has access, but which does not pertain to a particular case. *Id.* This definition is useful in two major respects. First, it is dynamic and allows flexibility in determining what is, or could be, a court record. In the same vein, it allows for the likely possibility that Maryland will institute an electronic filing system and deals with the treatment of those records. Second, it clearly delineates between records in connection with a case and records maintained at the courthouse or records to which a court has access.

listing the general policy objectives of the committee,[135] the committee recommended that, generally, access to public records should be the same no matter if the record is electronic or paper, or if the record is for a civil or a criminal trial.[136] Access to records, however, would not be limitless. As case files become available in electronic form, certain information, such as credit card information and medical records, should not be accessible online.[137] The guidelines set forth in this report attempt to balance the public's right to know with an individual's right of privacy in a manner that is workable and efficient. In certain areas, though, the guidelines do not go far enough. For instance, protecting individuals' identities in family proceedings should be seriously considered. However, the guidelines do take an initial step and set forth rules to be later adopted by the courts or the legislature.

At this time, neither the federal government nor state governments have taken sufficient measures to protect citizens from the dissemination of personally identifying information in court documents via the Internet. Although model suggestions have been proposed,[138] these changes have been slow to take effect. Social Security numbers, bank account numbers, and other similar information are currently required information in many federal and state actions. This information must be protected in order to prevent it from falling into the wrong hands, and legislation protecting such information must be implemented quickly.

---

[135] *Id.* at 5. These objectives include: benefit of public access, maintaining the role of the judiciary, promoting government accountability, contributing to the safety of the public, avoiding harm to individuals, increasing customer service, protecting trade secrets and other important business information, and avoiding the placement of undue burdens on the judiciary. *Id.*; *see also infra* notes 164–70 (discussing the policy objectives for the model rules of court access).

[136] Alpert, *supra* note 131, at 6.

[137] *Id.* at 11. Guideline 3(c) notes that such personally identifying information has such "remote" value to a case that the interest in protecting an individual from harm outweighs any benefit to public disclosure. *Id.* However, certain identifying information, such as name, address, date of birth, height, weight, sex, and race, and descriptions of events should not be kept confidential, except as mandated by statute or by court sealing rules. *Id.* The comment to Guideline 3 was intentionally drafted using broad language so that courts could promulgate more specific rules as needed. *Id.* at 11–12. Furthermore, it is uncertain whether Guideline 3(c) would require lawyers or court officials to redact certain identifying information in both the paper copy and in electronic form, or just the electronic form. *See also* CATE & VARN, *supra* note 37, at 19 ("Anonymous and pseudonymous records pose no meaningful threat" to individuals.).

[138] For more information on the effectiveness of model rules, *see infra* section V.

IV. THE EXTENT TO WHICH THE FEDERAL CONSTITUTION PROTECTS PRIVACY

Individuals who have been harmed by the dissemination of sensitive information via the Internet have tried to rely on the federal Constitution as grounds for a cause of action for the invasion of privacy. Although the right to privacy is not specifically mentioned in the Constitution, the Court's jurisprudence first established a right of privacy in areas such as personal choice to use contraception[139] and the ability to obtain an abortion.[140] The Court, then, in *Nixon v. Warner Communications, Inc.*,[141] noted that the public has a right to inspect and copy public records;[142] however, this right was never meant to be absolute.[143] The *Nixon* case, though, did not directly deal with the question of whether a person had a privacy right to his or her personal information.

The Court later addressed the issue of privacy interests in personal information in the landmark case *Whalen v. Roe*.[144] In this case, the Court noted that the right to privacy did not only include the personal decisions at issue in *Roe* and *Griswold*, but also included the protection of personal information.[145] Although the Court ultimately upheld the New York statute requiring physician

---

[139] *See* Griswold v. Connecticut, 381 U.S. 479 (1965); *see also* Eisenstadt v. Baird, 405 U.S. 438 (1972).

[140] *See* Roe v. Wade, 410 U.S. 113 (1973).

[141] 435 U.S. 589 (1978).

[142] *Id.* at 597 ("It is clear that the courts of this country recognize a general right to inspect and copy public records and documents, including judicial records and documents."); *see also* Solove, *supra* note 14, at 1157 (noting that the Court presumes openness to promote "transparency," or the ability for the public to keep watch over the government to ensure that it is acting properly).

[143] *Nixon*, 435 U.S. at 598. As supervisor of their own records, individual courts should determine when documents should not be released to the public. Records should not be released to the public in instances in which the files might "become a vehicle for improper purposes." *Id.* Examples of improper purposes include libelous statements that will be released by the media over a broad public and information that would hurt the business of one of the litigants. *Id.*; *see also* Solove, *supra* note 14, at 1157; Victoria S. Salzmann, *Are Public Records Really Public?: The Collision Between the Right to Privacy and the Release of Public Court Records Over the Internet*, 52 BAYLOR L. REV. 355, 362 (2000).

[144] 429 U.S. 589 (1977).

[145] *Id.* at 599–600. At issue was a New York law that required physicians to forward to the state the names of patients who are prescribed certain prescription drugs commonly sold on the "black market." *Id.* at 592–93. The plaintiffs, a minor patient and his father, argued that the "zone of privacy" extends to two distinct interests: "[o]ne is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions." *Id.* at 599–600 (citations omitted).

disclosure of patients prescribed certain medications,[146] the Court responded to the privacy issue by stating:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of . . . social security benefits, . . . and the *enforcement of the criminal laws* all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid *unwarranted disclosures*. . . . [I]n some circumstances that duty arguably has roots in the Constitution. . . .[147]

Thus, the Court acknowledges that, at times, people may have a constitutional right to privacy that outweighs the presumption of open access. It is interesting to note that the Court only specifically mentions criminal court documents;[148] it is unclear whether the accumulation of civil case files would warrant the same amount of protection. In either instance, the disclosure would have to be "unwarranted," and the Court never defines this vital term.

Although the Court recognizes a possibility of a right to informational privacy, individual courts may initially restrict public access in the interest of privacy. In one line of cases, the Court has repeatedly held that members of the media cannot be sanctioned for publishing information found in the public record.[149] In a complementary line of cases, the Court held that individual courts can either selectively grant access to records or condition the receipt of discovery information on a promise not to disclose the information to the media.[150] Based on these two premises, Professor Solove contends that although there is little

---

[146] *Id.* at 603–04.

[147] *Id.* at 605 (emphasis added); *see also* United States Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 763 (1989) ("[B]oth the common law and the literal understanding of privacy encompass the individual's control of information concerning his or her person.").

[148] There are competing views about whether criminal records should be afforded more or less protection. Maybe criminal case files should be afforded more privacy because they undoubtedly contain more personal information, such as age, race, criminal records, and more embarrassing information, such as the details of a crime, than civil cases. *See* Solove, *supra* note 14, at 1147–48 (aside from the above classes of information, criminal records often contain information about a defendant's social history, character, education, employment, income, medical and psychological information, as well as information about the victim). However, these files have a longer history of being open documents.

[149] *See* Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975); Oklahoma Publ'g Co. v. Dist. Court, 430 U.S. 308 (1977) (per curiam); Smith v. Daily Mail, 443 U.S. 97 (1979); Fla. Star v. B.J.F., 491 U.S. 524 (1989); *see also* Solove, *supra* note 14, at 1206–07.

[150] Solove, *supra* note 14, at 1207 (citing Los Angeles Police v. United Reporting Publ'g Co., 528 U.S. 32 (1999) and Seattle Times Co. v. Rhinehart, 467 U.S. 20 (1984), respectively).

personal protection for information that is already on public record, courts have some flexibility in determining whether or not the information should be public in the first instance.[151] Indeed, allowing the courts to either disclose information on a limited basis or not at all appears to be a viable option for safeguarding the privacy rights of individuals who could be harmed by public exposure.[152]

V. PROPOSED SUGGESTIONS TO BETTER PROTECT INDIVIDUALS' RIGHT TO PRIVACY

As shown above, the dissemination of court documents over the Internet poses the threat that individuals' right to privacy may be violated when sensitive, personally identifying information can be remotely accessed.[153] In order to curb the potential abuses of this information, especially the threat of increased identity theft, many judges, lawyers, legislators, and scholars have proposed potential solutions. These solutions must deal with four major issues: (1) types of information that should remain private; (2) differences, if any, between paper and electronic records; (3) ease of implementation; and (4) enforcement of the proposed standards. Thus far, the major proposed solutions include (in order from easiest to most difficult to implement):[154] issuing an increasing number of protective orders in individual cases; proposing model rules to deal with privacy issues; amending a jurisdiction's court rules to reflect privacy interests; enacting state and federal laws that would state what information cannot be disclosed, electronically or otherwise; and amending the federal or state constitutions to include a right to informational privacy. However, none of these current solutions

---

[151] *Id.* at 1212. Professor Solove classifies disclosure as either "pre-access" or "post-access," where pre-access means a disclosure made prior to it being placed on the public record and post-access means a disclosure made after it was placed on the public record. Because there is virtually no sanction for reporters who disclose information in the public record, post-access disclosures are constitutionally protected by the First Amendment. However, if a court can disclose information on the condition that it is only being used for certain purposes, the individuals mentioned in this record would have a greater privacy interest than would the public asserting an access interest. *Id.*

[152] A better argument may be made that Internet dissemination of all court documents violates a state right to privacy. See *supra* note 10 for a listing of all states with explicit rights to privacy in their constitutions. However, in order for a state supreme court to determine that rights to privacy have been violated, the court must also be willing to determine that the current public access or open record laws of the state are unconstitutional either facially or as applied. Given that each state has a long history of allowing open access, this is a difficult challenge. See *supra* note 68 for a listing of each state's public records acts.

[153] *See supra* Part II.

[154] Each system will have different difficulties, and this ordering of designs is merely a rough estimate of how easily or likely each one could be implemented. Certainly others may disagree and find that any one of these designs is either more or less difficult to implement than another.

is without flaws. Therefore, this Note proposes a solution that is relatively easy to implement, that protects individuals from releasing personally identifying information in public records, and that gives individuals a cause of action for damages incurred as a result of this loss of privacy.[155]

A. *Greater Use of Protective Orders*

The least involved way to protect privacy interests would be to encourage judges to issue protective orders over court documents. Judges would simply use the existing structure to better guard against the invasion of an individual's privacy.[156] Many who support increased access to judicial records endorse this position, noting that the system already contains the necessary procedural safeguards.[157] All jurisdictions have procedures to protect records, many of which are based on Rule 26(c) of the Federal Rules of Civil Procedure;[158] however, the protected materials are limited to information gathered through discovery, and the rules do not cover pleadings, motions, or briefs.[159] However, reliance on the current rules to protect documents and seal records is not enough. The status quo is not sufficient, and the system would greatly benefit from increased safeguards against the publication of sensitive material. One variation on this theme could be to have two levels of protective order: the current Rule 26(c) for prohibiting total dissemination, and a lower standard for keeping documents off of the Internet.[160] This idea protects privacy more, but it results in treating online documents and "hard copy" documents in different manners. As jurisdictions increasingly move

---

[155] *See infra* Part VI.

[156] Judges could use the rules of Civil Procedure to issue protective orders or to seal documents at any time during litigation.

[157] RAUL, *supra* note 17, at 71 ("Courts and judges have long experience with sealing court documents whose disclosure is inappropriate."); Vock, *supra* note 12, at 1. Groups that are in support of access, most notably journalists, are quite obviously drawn to this type of reform. Although this solution has the potential to protect privacy, journalists might be motivated more so by their want of continued access to information than in helping those in vulnerable situations.

[158] FED. R. CIV. P. 26(c). Rule 26(c) states that a party may move the court to restrict the use of discovery materials when "justice requires to protect a party or person from annoyance, embarrassment, oppression, or undue burden . . . ." Although the use of protective orders can be useful in the realm of discovery, the most damaging information is often found in pleadings, motions, and attorney briefs, rather than in depositions or documents. The scope of protective orders would have to be enlarged to deal effectively with these other court materials.

[159] *Id.*; *see also* Kaplan, *supra* note 13, at 3 (explaining that in the discovery stage, all that is required to obtain a protective order is "good cause.").

[160] *See* Kirby, *supra* note 1, at B1. According to clinical director of the Stanford Law School's Center for Internet and Society Jennifer Granick, in some cases "it would be wise to have a lower standard than the one for filing under seal, which would keep certain documents or information offline." *Id.*

to online filing, the originals will be in electronic form, and there will be no difference between the original and electronic forms, leaving a distinction without a difference.

B. *The Institution of Model Rules as Guides for Future Federal or State Legislation*

Proposing model rules would encourage each locality to determine its best course of action. The Judicial Conference, a joint effort between the National Center for State Courts and the Justice Management Institute, released a draft set of model rules in February 2002,[161] and a final report in October 2002.[162] The committee intended to guide states as they attempt to retool their own public access laws.[163] These rules begin by listing the conflicting goals that the commission tries to reconcile,[164] and by defining "court record" broadly to include all documents in connection with a case.[165] These rules, unlike most state

---

[161] Askew, *supra* note 1, at 5. This coalition drafted model rules on behalf of the Conference of Chief Justices and the Conference of State Court Administrators. A copy of these proposals can be found at www.courtaccess.org. Further information can be found at www.uscourts.gov/privacyn.pdf.

[162] *See* www.courtaccess.org/modelpolicy (last visited Jan. 21, 2004).

[163] Martha Wade Steketee & Alan Carlson, *Developing CCJ/COCSA Guidelines for Public Access to Court Records: A National Project to Assist State Courts* vii (2002), *at* www.courtaccess.org/modelpolicy/18Oct2002FinalReport.pdf. Each rule is accompanied by extensive commentary to guide states in formulating and enforcing their own access rules. The committee makes special note of the issues that it declined to address.

[164] *Id.* at 4. The goals listed include: maximizing accessibility to court records, supporting the role of the judiciary, promoting government accountability, contributing to the public safety, minimizing the risk of injury to individuals, protecting privacy rights and interests, protecting proprietary business information, minimizing any reluctance to utilize the courts for dispute resolution, effectively using the court and clerk of court staff, providing customer service, and preventing burdens on the court system. *Id.* Note that these policy reasons are largely the same as those Maryland listed as its policy objective. *See supra* note 135.

Professors Cate and Varn suggest twelve factors that should be considered when drafting legislation dealing with public records. Those factors are: (1) policymakers should identify and evaluate conflicting interests, (2) privacy solutions must respond reasonably to problems, (3) limits on access to protect privacy should be no more restrictive than necessary, (4) privacy interests are limited to personally identifiable records, (5) enhancing state revenue is not a privacy problem, (6) public information policy should promote robust access, (7) there should be no secret public records, (8) not every privacy/access issue can be balanced, (9) systems for accessing public records, and controlling their use should not be burdensome, (10) information must ensure the security of the public record infrastructure, (11) education and an informed citizenry, and (12) the process for balancing access and privacy should be sound. CATE & VARN, *supra* note 37, at 5–7 (1999).

[165] Steketee & Carlson, *supra* note 163, at 12. "Court records" are defined as:

court rules or statutes, specifically define records "in electronic form."[166] Generally, public access should be presumed,[167] but there should be a distinction between paper and electronic documents.[168] The provisions allow individual states to designate that certain documents can only be accessed at the court facility.[169] Furthermore, the rules would allow the redaction of certain, personally identifying information; however, individual lawyers carry the burden of ensuring that privacy is protected. [170] These model rules are flexible and give states latitude

---

(1) Any document, information, or other thing that is collected, received, or maintained by a court or clerk of court in connection with a judicial proceeding;

(2) Any index, calendar, docket, register of actions, official record of the proceedings, order, decree, judgment, minute, and any information in a case management system created by or prepared by the court or clerk of court that is related to a judicial proceeding; and [certain "administrative records"].

Id. The commission specifically does not include information exchanged between the parties without ever passing through the hands of the court, such as discovery documents. *Id.* at 12, 15.

[166] *Id.* at 20. A record "in electronic form" includes:

(a) electronic representations of text or graphic documents;

(b) an electronic image, including a video image, of a document, exhibit or other thing;

(c) data in the fields or files of an electronic database; or

(d) an audio or video recording, analog or digital, of an event or notes in an electronic file from which a transcript of an event can be prepared.

Id.

[167] Steketee & Carlson, *supra* note 163, at 22. The rules further mandate that individual districts cannot promulgate more restrictive access rules than the state. *Id.* at 24. This restriction on local court autonomy is to create equal access to public records throughout the entire state.

[168] *Id.* at 27. Documents that should be readily accessible remotely include party names, indexes of cases, lists of new cases, a register of documents filed in a case, calendars, dockets, and judgments or orders affecting the title of real property. *Id.* These documents only contain the basic information to a case and outline the steps that have been taken in a case. They do not reveal any of the substance of a particular case.

[169] *Id.* at 39. The rule does not list what materials should not be available online, but in the comments section, the committee suggests that the list could include addresses, social security numbers, family law proceedings, obscene exhibits, victim photographs, medical records, and the names of minor children, to name a few. *Id.* at 40.

[170] *Id.* at 45. The rules would allow certain information to be completely confidential in specific circumstances. The protected information could be specific information contained in a document or entire documents. Information that might fall within this category include social security numbers, tax returns, health information, juvenile information, family law case materials, and criminal case materials. *Id.* at 45–50.

Bankruptcy records are of special concern to the courts and to practitioners because the bankruptcy documents not only reveal personally identifying information, but also extensively list the debtors' assets and liabilities. *See, e.g.*, Mary Jo Obee & William C. Plouffe, Jr., *Privacy in the Federal Bankruptcy Courts*, 14 NOTRE DAME J. L. ETHICS & PUB. POL'Y 1011,

in drafting their own statutes, and they potentially protect a substantial amount of personal identification. However, they contain two fundamental flaws. First, the rules would be the delineation between records that can be accessed electronically and those accessed at court. As stated above, the rise of electronic filing may eliminate any differences between paper and electronic files. Second, the model rules provide no means for enforcement. If adopted, individuals could not receive redress for the harm caused by the online dissemination of sensitive information.

C. *The Implementation of State Legislation*

Another possible solution would be for individual court districts to adopt rules applicable in its jurisdiction. Maryland is currently attempting to implement general rules under which individual courts could promulgate specific rules.[171] Although allowing courts to design their own policies on privacy and access to court information might be a relatively easy way to achieve the court's objectives, there are two major flaws in this plan. First, each jurisdiction is likely to have different rules, potentially leading to forum shopping and unequal access to records. Second, without state legislation setting the basic guidelines, these rules may be contrary to public access laws.

The federal government and individual states could try to pass legislation setting forth either general policy considerations on the issue of privacy and open access or specific rules regarding permissible dissemination of court records. The United States Senate recently proposed a bill that would prohibit the use of social security numbers on court documents.[172] However, the bill was never referred to

---

1020 (2000). In its June 26, 2001 report, the Judicial Conference Committee on Court Administration and Case Management recommended that the social security numbers of debtors should be redacted with the exception of the last four digits. JUDICIAL CONFERENCE ON COURT ADMINISTRATION AND CASE MANAGEMENT, REPORT ON PRIVACY AND PUBLIC ACCESS TO ELECTRONIC CASE FILES App. A6 (June 26, 2001), *available at* http://www.uscourts.gov/Press_Releases/att81501.pdf.

[171] Alpert, *supra* note 131, at 1. The Maryland Commission recognizes that the legislature would have to enact statutory provisions protecting court documents from open access laws before the courts could promulgate rules to that end. The Commission, though, appears to intend that the state statutes would be of a general nature and that the individual court rules would deal with the particular details regarding informational privacy. At this time, the Commission's main objective is to start the process and give recommendations to the courts at a very general level, and to encourage districts to begin to consider these privacy concerns. *Id.*

[172] Democratic Senator Dianne Feinstein revived two bills on identity theft and social security numbers. Chloe Albanesius, *Security, Privacy, Wireless Issues Focus of New; Legislation*, NAT'L J. TECH. DAILY, Jan. 31, 2002. Senate Bill 223 would increase the penalties for those who commit identity theft, and Senate Bill 228 would prohibit the use of social security numbers on many government documents including drivers' licenses and court documents. *Id.*

a committee.[173] Florida currently addresses privacy and Internet access in its statutes,[174] and Ohio is considering legislation that would create a scheme to protect personal information in public records.[175] Passing federal and state legislation would give each citizen an equal right to access and protection of privacy within the law's jurisdiction, and in this respect, would accomplish more than an individual court district could do on its own. Perhaps the biggest challenge to a state or federal law would be a challenge under the First Amendment.[176]

D. *Amending Federal and State Constitutions*

The most lasting, and most difficult way to implement privacy laws would be to amend the U. S. Constitution and state constitutions. Amendments to the U. S. Constitution require an affirmative vote by three-quarters of all of the states or by a two-thirds supermajority of each house of Congress.[177] Although amendments to state constitutions are usually less difficult, amendments happen relatively infrequently. The reason that these changes are lasting is that amending the amendments will also be an extensive process.[178] At least one commentator endorses constitutional amendment as the only effective means for changing

---

[173] *See* H.R. TRACKING REP. NO. 108-228, at 1 (2003), LEXIS. Virginia, however, recently did adopt legislation that prohibits personally identifying information from being placed in documents that can be viewed through the Virginia court web sites. These limits apply equally to court documents and other records maintained on the web site, such as property deeds. Alan Cooper, *Curbs on Court Web Site Passed; Bill Limits Access to Personal Data*, RICHMOND TIMES-DISPATCH, Feb. 21, 2003, at A6. *But see* Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 109 (2001). Professor LoPucki argues that prohibiting the use of social security numbers in all instances would merely give rise to new forms of identification, giving those who would commit identity theft a new object to obtain. This argument does make sense in situations in which people must be identified by one method or another. However, in the context of court documents, social security numbers are not necessary for identification purposes, and the use of such numbers is often inconsequential to the legal proceedings. *Id.*

[174] *See supra* notes 87–91 and accompanying text.

[175] *See supra* notes 85–86 and accompanying text.

[176] The current Court probably would not give the media a right to access these "pre-access" documents based on the decision in *Seattle Times Co. v. Rhinehart*, 467 U.S. 20 (1984). Even if the chances of reversing these privacy laws may be slim, media will certainly bring challenges to the new laws.

[177] U.S. CONST. art. V. This difficult process has only been successfully completed twenty-seven times in the history of the United States.

[178] Constitutional amendment is an inflexible method of regulation. Because the issue of technology is one that changes quickly, amendments might not be the most efficient means of solving this problem. *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1543 (2000). It is possible that in the time necessary to amend a constitution, a new constitutional amendment would be needed.

privacy rights.[179] A constitutional amendment would effectively deal with any problems individual pieces of legislation might encounter. However, changing constitutions is never enough. The federal government and state governments will have to pass legislation in accordance with the new constitutional amendments to create specific, workable rules. The process of ratification plus passing legislation would be too time consuming and too inflexible, and thus it is not the most viable solution.

VI. A NEW MODEL FOR REGULATION AND ENFORCEMENT

The lack of privacy laws to protect an individual from the publication of his or her personal identifying information in public court documents subjects individuals to an unjustified risk of harm. Information, such as social security and credit card numbers, that falls into the hands of "bad actors" or even "nosey neighbors" could potentially leave people bankrupt and embarrassed.[180] The threat of harm is real; the number of incidents of identity theft and related crimes has greatly increased since the advent of the Internet.[181] The current state of open access laws permits too much damaging information to be accessed on the Internet from the privacy of individual homes.

As a result, the federal government and states need to pass legislation specifically dealing with access to private information in public court documents. The legislation should treat electronic and paper documents in the same way in the wake of increased use of online filing.[182] Furthermore, the legislation should completely ban the use of social security numbers; bank account numbers; credit card numbers; driver's license numbers; addresses; and the full names of people involved in family matters, such as divorce, custody, and adoption, because this information is particularly harmful if disclosed.[183] Individual states could classify

---

[179] Elbert Lin, Note, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1154 (2002). Lin's suggestion for a constitutional amendment would cover all uses of information over the Internet, not only the regulation of court documents. *See id.*

[180] *See supra* Part II.A.

[181] *See supra* notes 16–20 and accompanying text.

[182] *See supra* notes 41–50 and accompanying text. With the increasing use and popularity of online filing and case management, it is entirely plausible that by the end of the decade, paper submissions will be a thing of the past. Paper copies of documents will merely be printed copies of the electronic originals. Therefore, the need to distinguish between paper and electronic documents in public record regulations becomes a distinction without a difference. Furthermore, personally identifiable information is harmful if it is disseminated in either print or electronic form. So, the arguments that apply for the redaction in electronic form apply equally for redaction in print form even with the phenomenon of "practical obscurity." See *supra* note 14 and accompanying text for a discussion of "practical obscurity."

[183] These categories of information are those commonly exempted or proposed to be exempted from court documents because of the particular harm that could fall onto a person if

information according to its potential dangerousness to the individual. For example, social security numbers and bank accounts could be automatically protected by legislation while other information would have to be protected by another means, usually by a protective order. Other personally identifying information, such as addresses and telephone numbers do not usually pose the same danger from dissemination as those categories of information previously mentioned, so the use of this information should not be prohibited. The use of any personally identifying information should be avoided if possible. However, if a particular case warrants the use of such information, the records should not be available for public viewing—in either print or electronic form—until the sensitive material has been redacted.

The responsibility for redacting sensitive information from documents should be placed primarily on the lawyers.[184] Lawyers should be responsible for redacting this information from documents that they file with the court. However, clerks of court must be responsible for redacting this information from any previously filed documents that might be accessed over the Internet. Thus far, this solution endorses the path chosen by states that have proposed or passed similar legislation. These states, though, have not sufficiently addressed the problem of enforcement.

Enforcement is an essential element to any legislation, and without enforcement provisions, even the most well-crafted solutions are meaningless.[185] This note recommends two different methods of enforcement. First, if an individual finds that her court documents contain personally identifying information, she should be able to petition a court for the removal of such information. This remedy should be available to anyone, regardless of whether the individual was harmed by the publication of the sensitive information.

---

this information comes into the hands of "bad actors." See *supra* note 91 and accompanying text for a discussion of the information exempted from the Florida proposal; see *supra* note 134 and accompanying text for a discussion of the information exempted from the Maryland proposal; and see *supra* notes 169–70 and accompanying text for a discussion of the information exempted from the Justice Committee model proposal.

[184] The responsibility for redaction lies primarily on the lawyers under the model proposal as well. *See supra* note 170 and accompanying text.

In September 2003, the judicial conference, headed by Chief Justice William Rehnquist, ordered that certain information, such as social security numbers, dates of birth, bank account information, and select family information, be redacted from online court documents. Dan Christensen, *Public Info or Online Menace?; Electronic Court Filings Prompt Identity Theft Fears*, CONN. LAW TRIBUNE, Nov. 17, 2003, at 1. However, the committee decided that attorneys should be responsible that this information does not end up on the Internet. If a lawyer forgets to remove this information, he or she could be liable for sanctions. *Id.*

[185] The problems associated with identity theft and embarrassment, see *supra* notes 16–20 and accompanying text, are so harmful that a rule with "teeth" is necessary. However, thus far, no set of proposed rules dealing with informational privacy of sensitive court information has included an enforcement scheme.

Second, a new cause of action against the attorney who placed the information in documents should be available for individuals who have suffered real, economic, or psychological harm from the dissemination of their personally identifying information.[186] For example, an individual who has become the victim of identity theft should be able to sue the lawyer who placed that information in a public document, even if that attorney was not her own attorney. This protection should also be available to victims of non-economic crimes, such as stalking or harassment commenced as a result of placing this sensitive information online. Under this recommendation, lawyers carry a heavy burden to ensure that this information does not become part of the public record; however, without an enforcement scheme, the legislation would have no real effect.

VII. CONCLUSION

The current system provides very little protection for individuals who are required to use personally identifying information in their court filings. Most state's public records laws became outdated with the growing popularity of the Internet and other means of electronic dissemination of records. Change must come quickly, and new legislation must be feasible to implement, accommodating to litigants who need the court to hear such information in particular cases, and court enforced. Until such legislation takes effect, individuals are unjustifiably placed in a position of harm.

---

[186] A separate cause of action already exists against the perpetrator of the crime. The actual wrongdoer can be tried in criminal court, and the victim could also sue in civil court. However, because the perpetrators of identity theft are rarely caught, *see supra* note 20, a separate cause of action is necessary against the lawyer who has proximately caused the harm.